Q1 : Implementation of RSA using 512 bit and 1024 bit parameters

```
+++,B180341CS_Prog1.cpp
```

Output :

```
➜  Submission git:(master) ✗ ./B180341CS_Prog1.out
[+] Using 512 bit keys
[+] Generated Keys :
N : 148486496290321545913325802424370498514688889219007315575671003825217510858297287200943395746083346293934093315360770346819690825194577741789644270658080537602607394645159974652313541074693626614717913497
576828299648544709138381964725902327564557166227004858075159318907612504786779336553132400878001972090881
E : 8881050184806893203567432503900729362600594380058293011560253768367898105960006694743410076281902765548459975245998560530373202138150806122160574391455218746813549411936567564442746564107833685658121970 73
16704783444810221323288232357671213477248136287022216473371675593819897066284616179540235073049436304875
D : 731519057743852848143014102132367180613584621407778823166381335774242137482715958312718301602821813061807507769327540407619961642530160565071433994745550110515954216995854113641838660699102808211044032705
79402162282115511285315274861402793945855702335860109758408471876291432992639464761936668837833720687555
--------------------------------------------------------------------------------
Message     : 2567
Encrypted   : 1171296768129141615865388103041993344748786970120433360541157926907061629435338246671501880720021924169438862409562267572686303165484099972121714824986072255741381668918220838379631148136374730 5
58378300131873061400547024431490408822478218722943884918122794657463266567646037243547661491816999962925352949 2406
Decrypted   : 2567
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
[+] Using 1024 bit keys
[+] Generated Keys :
N : 1631951807135047098229024602736158534916292766189976416786458085731822081107097673789302273921183280099875687479469979961279083178068633844488648200622353655484652916960709948050834944095783725525226614 85
6118979339537585099778748948976361281918247460472490462601604873593136927925561038178187685627169582839267095531254209957903425816564974355013360356054602656238741376931667770132908709441159713850254035278362
1715384025768503850778222895891195282231637172826226625155156302910457632793931225167821133012459588523905078040360801518132415273693933855598671837736144929816928214761194673534850426042373659350873499181
E : 1377302229747412426624002946092823690017993081761601484105414014197949400254594413023060977909455694236600063240416266594531110487860696125595119295131996387730345578316664622067234308041183149414461084641
9016255113133629783536910506035223662104306733376167130999922767132389437506306266886908017183443558326577013401624000863066123965507990002913137462901264852079779496253822963271986198938664937091894385861241
7941619331639855298559759631333843265082206955423530274149363151861766947988451067626154394707629081563233645952593025455917599210008687905499742516528481167912790317246077430881067576101497085746778620419
D : 1480825894778572309106928590018681824326547726380061360865348980295088910552867901095854905020667923184891261358537115768506516194236696516849783826223023769925386007206504884535912271775210273062979468 14
8713615095901081671677701263962420531368870485306992255668115768065757273990668909484996733987920039247525328717858899682522809087711862421183783954880716950571880893721538055197590414631614484002492369725558
8659575171855708867241882923125636397824598014526589776388704013817714563003507749914786823041482740707660303153086523900322006405986756653499545117342197007381297064866829525122697131302321300825861787019
--------------------------------------------------------------------------------
Message     : 123456
Encrypted   : 87768871075622783869745788991910171812871895823992236525183014282569654906390148661087446236339196192236655892806883012459179781309691761724113452344535432491548185214643670001538485980999967880
3566858273665252677286949258942758474111190238814321507589488177768269153009172876129163360323941185144421491284521558542957315482034619669589426106861291073370508024159406963885270835961930106994431556438925
6039430967592631107282572544680858030885112756616115851428575725474330881797030934928846488471571249249082205364377879377508987917500549454323563457686257610538456605191698587211577336990693176162543148771963
411719
Decrypted   : 123456
--------------------------------------------------------------------------------
```

Q2 : Implementation of ElGamal using 512 bit and 1024 bit parameters

```
+++,B180341CS_Prog2.cpp
```

Output :

```
➜  Submission git:(master) ✗ ./B180341CS_Prog2.out
[+] Using 512 bit keys
P   : 20680801447346411027229513082662769669814409687582262090019855061319661143717987841759608215835666205892297694798351975528004424098079811517090491726974287
Q   : 10340400723673205513614756541331384834907204843791131045009927530659830571858993920879804107917833102946148847399175987764002212049039905758545245863487143
G   : 11507791256096358033151250820527189901268261577138874908350569928558210625844973297277567412059017764658250004292533286127558799374617581665665126154641974
----------------------------------------------------------------
Keys
X   : 149286813434057961744436951517757813875149685526750820844685418409252544830758028711568437339305084291807014722497820861743323892611597410365149180968552
Y   : 65585044746029987448870375384137053504690880168863978886270141839019302957861403909771031721006468204289107927799543077687945070330598830365600406666618406
----------------------------------------------------------------
Message
2567898
----------------------------------------------------------------
C1  : 53330671310784365493500155571451326506605643368553785493227364010731986532447378495302853866685711417501035568715834493131559002262142213683885377609145 37
C2  : 14063278002317330792328020246098045841928285245838382575131919296099102651384960507744085601296462064388869473764474642219312708686091968732498629302195566
----------------------------------------------------------------
Decrypted Message   : 2567898
----------------------------------------------------------------
----------------------------------------------------------------
[+] Using 1024 bit keys
P   : 1929447009107974818814845644596144535755807572590465908998428478496663623897626345247935758843970942279231834561862690934545497873959916103808687997470087612072643118667550366429128337276911964521909813
67493234240862622209171682527065210263083968912547252326354109731597986940687475525466116066848040262091119
Q   : 9647235045539874094074228222980722678779037862952329544992142392483318119488131726239678794219854711396159172809313454672727489369799580519043439987350438060363215593337751832145641686384559822609549068
3746617120431311104585841263532605131541984456273626163177054865798993470343737762733058033424020131045559
G   : 4252936356811906642986358601111530034557655458773409097526818622112987681665028271707876364269534293012772807085747887610928836068933736255915169328414877843269675018647543042564777331007857841495391228
2473479264521027523925317077626790709072523646618091220199771369768677737451050612755380062279967501891593
----------------------------------------------------------------
Keys
X   : 1531566496072318555728273593927241531193239061201165383595759027012151755831829819361057331266502918332538506324855980350139307642039701638529964933396101632195259200646485226548461986856920572327078460
1118477974524180044107022804007560082003088351807956291251025842139323616698303610942003236439195603408091
Y   : 1179747257505156189412004873689114095894236293663560609963114915414885566580875416833193021573863750313125349748662266939111082906356332696363928582436537915700451052311182392334266748144741702030991712
13263986946952644351427920295336893406330497795292834650146707613767633352753661084277004997058722955374614
----------------------------------------------------------------
Message
54321
----------------------------------------------------------------
C1  : 1320759589413237572594252527608828898835801121266242771180523476353195612959455089913737896762984070688965549928689465908296774970086938816466346057451552478300823205396529650132791312283503772161091127
78916686236672692909316517422006858306802262494810915260286540609711432279884739034635202449960449454550733
C2  : 1750066448615721858252120287508221173196326282059644434318068132063375326922123128406933934228873026321207753958180083327879269171928140215867150167565095509179980760795403375112589549921130917680737835
30105331448199439192176883523599134728216507928151613561236932039710354314472924242968460101446219231921046
----------------------------------------------------------------
Decrypted Message   : 54321
----------------------------------------------------------------
----------------------------------------------------------------
```

Q3 : Implementation of ECC using F-192 parameters

```
+++,B180341CS_Prog3.cpp
```

Output :

Q4 - a : Digital Signature Implementation using RSA

Header Files with Necessary Utils for SHA Hash

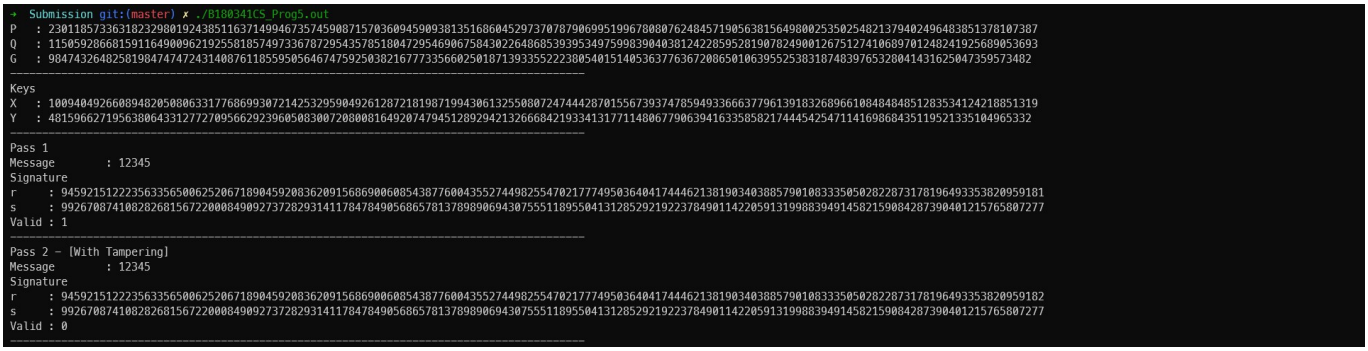
```
+++,B180341CS_Prog4.cpp
```

Output :

Q4 - b : Digital Signature Implementation using ElGamal

```
+++,B180341CS_Prog5.cpp
```

Output :



Q4 - c : Digital Signature Implementation using ECC

```
+++,B180341CS_Prog6.cpp
```

Output :

```
➜  Submission git:(master) ✗ ./B180341CS_Prog6.out
Actual Message :
4321
-----------------------------------------------------------
Encoded Message :
Point(5332114,14931131042217044422775530438947894543253637772660042561l7,627710173538668076383578942320766641608390870039032496l279)
-----------------------------------------------------------
Alice Keys :
27355195046470119052556055556767630515561224870037731499938
Point(17998062770722594967022250005576530023767413833192531499885,43028715511661111842030849518621790591450911129380842580940627710173538668076383578942320766641608390870039032496l279)
-----------------------------------------------------------
Bob Keys :
13625820429854675434551446789791741681968320450595557129780
Point(26963601463833796487669200384577286112443686881259812947460877576746360774864108816629920251935630705606935267342565,627710173538668076383578942320766641608390870039032496l279)
-----------------------------------------------------------
Session Key :
626870982904803135537081524410822875193280065822842639676l
-----------------------------------------------------------
Pass 1 :
Signature :
r    : 97981334956896744056207353584220764894798255814182567332
s    : 42679932363575151117083795171729120809221181750690085178790
Valid   : 1
-----------------------------------------------------------
Pass 2 - [With Tampering]
Signature :
r    : 97981334956896744056207353584220764894798255814182568566
s    : 42679932363575151117083795171729120809221181750690085178790
Valid   : 0
-----------------------------------------------------------
```